U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
OCT 31 2017
CLERK, U.S. DISTRICT COURT
By _____ Deputy

UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with email addresses: hindi14@yahoo.com, hindi.14@yahoo.com and tony.hindi@yahoo.com

Case No. 4:17-MJ-841

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Information associated with email addresses: hindi14@yahoo.com, hindi.14@yahoo.com and tony.hindi@yahoo.com as described in Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251, 2252 and 2252A and 2422	Possession, receipt, production, distribution of child pornography, coercion and enticement

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

LeAndrew J. Mitchell, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/31/17

Judge's signature

City and state: Fort Worth, Texas

Jeffrey L. Cureton, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, LeAndrew J. Mitchell, being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI), and I have been employed in this capacity since December 2008. I am a graduate of the Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.). I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

2. As part of my duties as an HSI agent, I investigate criminal violations relating to the sexual exploitation of children, including the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2422, 2251 and 2252. I have received training in the areas of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

3. This affidavit is being made in support of an application for a warrant authorizing the search of the records associated with the email addresses **hindi14@yahoo.com, hindi.14@yahoo.com** and **tony.hindi@yahoo.com**, stored at the premises owned, maintained, controlled, and operated by Yahoo Holdings, Incorporated (hereinafter, "Yahoo"), headquartered at 701 First Avenue, Sunnyvale, California. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo to disclose to the Government records and other information in its possession pertaining to the subscriber or customer associated with these accounts, including the contents of communications, which represent evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A.

4. The statements included in this affidavit are based in part on an investigation I have conducted, as well as information provided to me by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me regarding this investigation. I have included only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A is currently stored in the Yahoo records associated with email addresses **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com**, more specifically described in Attachment A incorporated with this affidavit.

5. I further submit that the information set forth in this affidavit establishes probable cause to believe that the individual using Yahoo accounts **hindi14@yahoo.com**,

hindi.14@yahoo.com and **tony.hindi@yahoo.com** has been involved in the production, distribution and receipt of child pornography, by coercing minor victims to produce sexually explicit content. Investigation into an instant messaging profile used by this individual revealed **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com** were provided as communication channels for the individual; therefore, the facts and circumstances set forth in this affidavit will show probable cause to believe these Yahoo accounts will have stored information and communications that are relevant to this investigation, including, but not limited to, the identity of the person controlling these accounts.

DEFINITIONS

6. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Internet Service Providers" (ISPs) are commercial organizations that provide individuals and businesses with access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet, including telephone based dial-up, satellite-based internet access, dedicated circuitry, or broadband-based access via a digital subscriber line (DSL) or cable television lines. ISPs typically charge a fee, based upon the volume of data, commonly referred to as bandwidth, in addition to the type of connection that the connection supports.

Many ISPs assign each subscriber an account name, such as a user name or screen name, as well as an email address and an email mailbox, and the subscriber typically creates a password for the subscriber account. By using a computer equipped with a telephone (dial-up) or cable modem, the subscriber can establish communication with the ISP, and can access the Internet by means of a combination of the user account name and password.

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

c. "Electronic Mail," commonly referred to as e-mail (or email), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. An Internet email message generally consists of three components: the message envelope, the message header, and the message body; in some cases, it may include a fourth component, an attachment.

Email attachments can include any type of digital file. There are numerous methods of obtaining an email account; some of these include email accounts issued by an employer or an education authority. One of the most commons methods of obtaining an email account is through a free web-based email provider such as, Microsoft, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account.

d. The term "communication channel" means a medium through which a message can be transmitted to its intended audience, such as print media or electronic media (e.g., oral communications or broadcast). In account subscriptions, it refers to a means of delivering account information or other messages to a customer, like email, telephone communication, or facsimile.

e. The term "sextortion" refers to a form of sexual exploitation and extortion that employs non-physical forms of coercion, such as blackmail, to acquire sexual content (e.g., sexually explicit photographs and videos), money or sexual favors from the victim.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or typing), or electrical, electronic, or magnetic form (including, but not limited to: tape

recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks or DVD's, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

INFORMATION REGARDING YAHOO MAIL

7. Yahoo is a U.S.-based multinational technology company that provides a variety of Internet related services and products. Examples of popular Yahoo services include Yahoo Mail, Yahoo Messenger, Yahoo Answers, Yahoo Finance and the Yahoo search engine.

8. Yahoo Mail is a webmail service that allows account holders to send, receive, and store emails and attached digital files on Yahoo's servers, or within other Yahoo Account service applications. Such emails and digital files can include photographs, videos, documents, email text, and structured data (i.e., contacts and calendar items). Yahoo subscribers may obtain email accounts with the "yahoo.com" domain name.

9. During the account registration process, Yahoo asks subscribers to provide basic personal information. Based on my training and experience in cybercrimes investigations, I am aware that Yahoo stores and maintains electronic communications and information about subscribers of their services, including their email service.

This information includes account access information, email transaction information, and account application information. This information may constitute evidence of the crimes under investigation as it may contain information that will identify the party in control of the subject account.

10. Yahoo allows account holders to access their files, which are stored on Yahoo's servers, from any digital device that can access the Yahoo account application's website (i.e., Internet accessible devices). Yahoo provides free storage, up to 1TB, that can be used to store content on any of the Yahoo applications, including Yahoo Mail. Based on my training and experience in child exploitation investigations, I am aware that evidence directly relating to who was using a specific Yahoo account may be found in the aforementioned information.

OVERVIEW OF INVESTIGATION

11. In October 2016, the Windsor Police Service (WPS) in Ontario, Canada, was contacted by the mother of a 12-year-old female, hereinafter referred to as Minor Victim 1 (MV1). The mother advised WPS investigators that in September 2016, MV1 had been forced to send sexually explicit images and videos to an unknown individual on Kik[1]. MV1's mother informed investigators that she observed a conversation between MV1 and this individual, during which the unknown subject threatened to post MV1's sexually explicit images on social media if MV1 did not send additional images.

[1] Kik is an instant messaging smartphone application that allows users to communicate without sharing a telephone number. Kik users can use the application to transmit messages, images, videos and other content with other users.

MV1's mother provided WPS the Apple iPod that MV1 was using to communicate with this individual, and granted consent for the contents to be searched.

12. In November 2016, a WPS computer forensics examiner searched MV1's iPod, and located a Kik chat with an individual using Kik username "cutegirl.e", display name "GIRLS ONLY". During this chat conversation, Kik user "cutegirl.e" demanded to receive access to MV1's email account, and threatened to expose "everything" online if she did not comply. The subject also sent MV1 a screenshot of several sexually explicit files of MV1, which appeared to be saved to a mobile device, and included a message that stated "I'm about to make video and upload it online and post the pic too". The WPS examiner determined several of the files sent by MV1 to this unknown subject satisfied the Canadian Criminal Code's definition of child pornography.

13. On November 23, 2016, WPS submitted a Canadian Production Order to Kik, requesting the subscriber information and contents associated with Kik account "cutegirl.e." On or about February 8, 2017, WPS received the first of two responses from Kik, which contained the subscriber information and part of the contents of the "cutegirl.e" account. Kik advised that the remaining data would be sent at a later date due to the large volume of data contained in the account.

14. On March 15, 2017, WPS received the remaining account information from Kik relating to the "cutegirl.e" account. WPS Constable Liyu Guan reviewed the Kik records, which included the following subscriber information:

Name: GIRLS ONLY
Email: hindi1666@yahoo.com[2]
Registration IP Address: 107.77.164.56
User Date of Birth: August 3, 1991
Registration Device: Samsung SM-N900T

15. Constable Guan reviewed the contents of the "cutegirl.e" account, and observed sexually explicit images and videos of several minor females between the approximate ages of 12 to 16 years old. Many of these files consisted of screenshots that depicted the victims, as well as text communications that indicate the minors were coerced into producing the illicit content by sextortion. Investigator Guan also observed approximately 29 sexually explicit files of MV1 within the account.

16. Kik records also indicated the profile picture for this account was uploaded from IP address 24.182.202.179. Log-in data further indicated this Kik account was accessed multiple times between August 2016 and November 2016 using this same IP address. Constable Guan researched this IP address, and learned that it resolved to the Fort Worth, Texas area. Because the user of this suspect account appeared to be located in the United States, WPS contacted the HSI Attaché office in Toronto, Canada for assistance with the investigation.

17. In August 2017, HSI Toronto reviewed the WPS case file, and forwarded the information to the HSI Dallas Child Exploitation Group for investigation. On or about September 1, 2017, HSI Dallas received the evidence relating to this case, which included the account records and contents for Kik user "cutegirl.e" obtained pursuant to the

[2] In October 2017, HSI served legal process on Yahoo for information regarding this account, and Yahoo advised that hindi1666@yahoo.com is not a valid email address at this time.

Canadian Production Order.

18 Beginning on or about September 5, 2017, I began reviewing the evidence relating to this investigation. During a review of the contents of the "cutegirl.e" Kik account, I observed evidence that indicates the user of this account was actively involved in the coercion and enticement, production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A. Screenshots found within the contents of this account indicate the user of this account coerced multiple female minors to produce sexually explicit images and videos, by threatening to post their pictures online, or by threatening to commit suicide if the minor did not comply. Two of the videos I observed in the contents of the "cutegirl.e" Kik account are described as follows:

File Name	Description
[redacted]a818	This file is a twelve-second video of MV1, who has been identified as a twelve-year-old minor female, masturbating in front of a restroom mirror.
[redacted]1b3b	This file is a one minute, twenty-four second video of a minor female between the approximate ages of 11 and 13 years old, who is nude from the waist down. During the video, the child masturbates on camera.

Based on my training and experience in child exploitation investigations, I submit that these files meet the federal definition of child pornography found in 18 U.S.C. § 2256.

19. The review of the "cutegirl.e" Kik account also indicated the user of this account communicated with other individuals involved in child exploitation violations.

Within the account records were screenshots that indicate the user of this account shared the pornographic images and videos of minors who failed to comply with his/her sextortion demands. Screenshots and Kik records indicate the user of the "cutegirl.e" account distributed child pornography to the victims and other individuals, on Kik and other Internet platforms, on multiple occasions.

20. On or about September 14, 2017, HSI served a subpoena on Kik for subscriber information and recent log-in data relating to Kik account "cutegirl.e." On or about September 15, 2017, Kik responded with the following subscriber information:

> Name: GIRLS ONLY
> Email: **hindi14@yahoo.com**
> Registration Device: Verizon SM-G920V
> IP Addresses: 24.182.202.179; 76.186.70.35

21. I subsequently researched IP address 24.182.202.179, and determined that this IP address is controlled by Charter Communications and resolves to the Fort Worth area. I also researched IP address 76.186.70.35, and determined that this IP address is controlled by Time Warner Cable and resolves to the Arlington, Texas area. On September 20, 2017, I served a subpoena on Charter Communications[3] for the subscriber information relating to the customers assigned these IP addresses at the times they were used to access the "cutegirl.e" Kik account. Additionally, on September 28, 2017, I served a subpoena on Yahoo for subscriber information relating to email address **hindi14@yahoo.com**, which was listed as the most current

[3] Due to recent business acquisitions and mergers, Time Warner Cable and Charter Communications are now doing business as Charter Spectrum. Charter is presently handling all legal process for both entities.

email address associated with the "cutegirl.e" account.

22. On or about October 1, 2017, Charter sent their first subpoena response, and reported that IP address 24.182.202.179 was assigned to the following subscriber when used to access the "cutegirl.e" account:

Subscriber Name: Stop N Shop Mini Mart
Subscriber Address: 2601 Riverside Dr., Fort Worth, TX
Lease Dates: November 11, 2015 to September 21, 2017

It should be noted that this IP address was also recorded in the original subscriber records obtained by WPS, referenced in paragraph 16 of this affidavit.

23. On or about October 5, 2017, Charter sent their second subpoena response, and reported that IP address 76.186.70.35 was assigned to the following subscriber when used to access the "cutegirl.e" Kik account:

Subscriber Name: Kharieh Hindi
Subscriber Address: 3211 W. Division St., Trlr. 209, Arlington, TX
Lease Dates: June 6, 2017 to September 22, 2017
Activation Dates: September 26, 2014 to present

24. On or about October 16, 2017, Yahoo complied with their subpoena and provided the following subscriber information for email address **hindi14@yahoo.com**:

Full Name: Mr Abd el-rahman
Alternate Communication Channels: **tony.hindi@yahoo.com**, **hindi.14@yahoo.com**
Telephone Number: (817) 308-7852
Account Created: January 11, 2009
IP Addresses: 76.186.70.35; 24.182.202.179

25. Open source and law enforcement databases indicate 3211 W. Division Street, Trailer 209, Arlington, Texas, is associated with the Hindi family (or Hendi, as some family members appear to use this spelling), whose adult members include S. Hendi, M. Hindi, Y. Hendi and K. Hindi. Records also indicate this family operates the Stop N Shop Mini Mart, located at 2601 Riverside Drive, Arlington, Texas. To date, HSI has not found records of a "Tony Hindi" residing at the Hindi residence or associated with the Stop N Shop Mini Mart; and, based in part on the erroneous and/or incomplete subscriber information for the aforementioned Kik and Yahoo accounts, the investigation into the subject involved in these child exploitation offenses remains ongoing at this time.

26. Based on my training and experience, I am aware that email is a popular method of Internet communication that is used by individuals involved in the sexual exploitation of children. For example, individuals involved in child pornography offenses often utilize email to share and store child pornography, and to discuss the sexual exploitation of children with other like-minded individuals. I am also aware that it is common for individuals, including but not limited to those involved in child pornography offenses, to maintain multiple email accounts for different purposes, and to send email messages from one personal account to another. When individuals maintain multiple email accounts, they often use similar usernames and passwords (e.g., **hindi14@yahoo.com** and **hindi.14@yahoo.com**) which are only distinguished by a few characters. This is likely done to make it easier for the user to create, maintain and access the various accounts.

27. The facts set forth in this affidavit establish probable cause to believe that the individual using email address **hindi14@yahoo.com** and Kik account "cutegirl.e" is accessing these accounts using the Internet services at the same two locations. Based on the investigation to date, I also have reason to believe that the usernames for email accounts hindi1666@yahoo.com, **hindi14@yahoo.com** **hindi.14@yahoo.com** and **tony.hindi@yahoo.com**, all stem from the surname "Hindi." Therefore, I submit that there is probable cause to believe that the email accounts to be searched will contain evidence, fruits and/or instrumentalities of violations of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A, including, but not limited to, the identity of the individual involved in these offenses.

CONCLUSION

28. Based on the information set forth in this affidavit, I respectfully submit there is probable cause to believe that 18 U.S.C. §§ 2422, 2251, 2252 and 2252A have been violated, and that computer systems under the control of Yahoo, Incorporated contain evidence and instrumentalities of these crimes. Specifically, there is probable cause to believe that the email accounts **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com** will contain evidence of these offenses, including, but not limited to, identification of the individual who controls these accounts. Accordingly, I request that this Court issue a search warrant requiring Yahoo to produce the records outlined in Attachment A, so that agents may analyze and seize the items outlined in Attachment B.

29. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

LeAndrew J. Mitchell
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on this 31st day of October, 2017 at 4:55 a.m./p.m. in Fort Worth, Texas.

JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to information associated with **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com** that is stored at premises owned, maintained, controlled, or operated by Yahoo Holdings, Incorporated, a company headquartered at 701 First Avenue, Sunnyvale, California.

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Yahoo to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Yahoo personnel by law enforcement agents. Yahoo, Inc. personnel will be directed to isolate those accounts and files described below;

2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files associated with **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com**, including an exact duplicate of all information stored in the computer accounts and/or files described below;

3. Yahoo system administrators will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;

4. Yahoo will disclose responsive data by sending to the following recipient using the U.S. Postal Service or another courier service, notwithstanding 18 U.S.C. §§ 2252, 2252A or similar statute or code: Special Agent Jason Mitchell, 125 E. John Carpenter Freeway, #800, Irving, Texas 75062.

5. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and

6. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator, and will not further review the original duplicate absent an order of the Court.

Attachment A

ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

Section I: Information to be disclosed by Yahoo

For each account or identifier associated with **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com**:

a. The contents of all emails stored in the account, from the time of account creation to present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The contents of all Instant Messages (IM) associated with the accounts, from the time of account creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. Any deleted emails, including any information described in subparagraph "a" above;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates,

account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

f. All content in the Docs, Calendar, Friend Contacts and Photos areas;

g. Any and all Yahoo IDs listed on the subscriber's Friends list;

h. All records pertaining to communications between Yahoo, Inc. and any person regarding the account, including contacts with support services and records of actions taken;

Section II: Information to be seized by the Government

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence and instrumentalities of violations of 18 U.S.C. §§ 2422, 2251, 2252 and 2252A, which make it a crime to coerce and entice, produce, distribute, receive, possess or access with intent to view, child pornography, including, but not limited to, **hindi14@yahoo.com**, **hindi.14@yahoo.com** and **tony.hindi@yahoo.com** information pertaining to:

a. The receipt, possession, access with intent to view, or distribution of email communications, photos, or visual depictions of minors. Furthermore, the receipt, possession, or distribution of personal identifying information and financial

account numbers, including, but not limited to credit card verification values (CVV) and names, addresses, dates of birth, and financial account numbers.

b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subject and any co-conspirators, the names, addresses, and locations of potential victims, and any disposition of the contraband regarding the crimes under investigation.

c. Records relating to who created, used, or communicated with the account or identifier.

Attachment B